

CLAIMS

1. An access control protocol between an electronic key (EK_{kj}) and an electronic lock (B_i) performing access control, in which protocol, following presentation of said electronic key (EK_{kj}) to said electronic lock (B_i), a random variable message (a_{ij}) prompting authentication of the electronic key (EK_{kj}) is transmitted from said electronic lock to said electronic key, characterised in that, on receiving said random variable message (a_{ij}) prompting authentication, the protocol consists of at least, in succession:

- calculating and transmitting from said electronic key (EK_{kj}) to said electronic lock (B_i) a digital signature value of said random variable message prompting authentication based on a private signature key (K'_s) and specific authentication data) said specific authentication data transmitted by said electronic key (EK_{kj}) to said electronic lock (B_i) consisting of at least one public key (K'_p) certificate associated with said private signature key (K'_s), said public key certificate consisting of a digital signature value of at least one validity time period (PH_j) relating to a right of access and of said public key (K'_p), said signature value being calculated from another private signature key (K_s) associated with another public key (K_p), and, after reception by said electronic lock of said signature value (C_i) and said specific authentication data (Da_i):

- verification (1003) $v_{KPK',P}((C_i, D_{aj}))$ by said electronic lock (B_i) of the authenticity of said signature value (C_i) as a function of said specific authentication data (D_{aj}) and, in response to a positive or negative result of said verification:

- acceptance or respectively refusal of said access.

2. A protocol according to claim 1, characterised in that said step of verification of said signature value

- verification (1003b) by said electronic lock (B_i) of said signature value (C_i) as a function of said specific authentication data (Da_i).

4. A protocol according to claim 2, characterised in that validity time period (PH_j) includes a plurality of non-contiguous time intervals.

5. A protocol according to claim 2 or claim 3, characterised in that each validity time period (PH_j) consists of at least one time interval having two limits each expressed as a date in terms of day, month, year and a time in terms of hour, minute, second.

6. A protocol according to any preceding claim, characterised in that said random variable message (a_{ij}) prompting authentication is a function of an identification value (C_i) of said electronic lock (B_i) and a continuously increasing variable value (CO).

7. A protocol according to any of claims 1 to 6, characterised in that, after reception of said random variable message (a_{ij}) prompting authentication by said electronic key (EK_{kj}) but before the step of calculation and transmission of a signature value (C_i) by said electronic key, said electronic key (EK_{kj}) having an internal clock, said protocol further consists of an auxiliary verification step (1007) for authorising

~~add~~
a

[illegible]